

AMENDMENT TO THE CLAIMS

1. (Currently Amended) A method for protecting data having an authentication phase comprising the following steps:

(a) providing a biometric feature;
(b) digitizing the biometric feature to create digitized biometric authentication feature data;

(c) decrypting an encrypted code word on the basis of the digitized biometric authentication feature data thereby obtaining a decrypted code word, and;

(e d) recovering secret data ~~by means of a decryption of from the decrypted code word on the basis of the digitized biometric authentication feature data~~ and on the basis of a coding-theory method with a correction capacity, the correction capacity being freely selectable.

2. (Previously Presented) The method according to claim 1 having an initialization phase comprising:

after providing a biometric feature, digitizing the biometric feature to create digitized biometric feature data;

providing secret data;

encrypting on the basis of the digitized biometric feature data and fault tolerantly coding the secret data.

3. (Previously Presented) The method according to claim 2 including using the consecutive steps:

fault-tolerantly coding the secret data to create a code word;

encrypting the code word on the basis of the digitized biometric feature data to create an encrypted code word.

4. (Previously Presented) The method according to claim 3, wherein the code word is generated by a generating matrix.

5. (Previously Presented) The method according to claim 2 including the step of creating initial correction data to describe the space of allowed code words.

6. (Previously Presented) The method according to claim 2 including the step of providing initialization correction data on the basis of the digitized biometric feature data.

7. (Previously Presented) The method according to claim 1 including the steps:

creating authentication correction data on the basis of the digitized biometric authentication feature data;

recovering the digitized biometric feature data on the basis of the authentication and initial correction data;

decrypting encrypted secret data on the basis of the recovered digitized biometric feature data.

8. (Previously Presented) The method according to claim 7, wherein the initial correction data are created by calculation of the digitized biometric feature data modulo n .

9. (Previously Presented) The method according to claim 7, wherein the authentication correction data are created by calculation of the authentication feature data modulo n .

10. (Previously Presented) The method according to claim 2, including using user-specific initial correction data and/or user-specific fault-tolerant coding.

11. (Currently Amended) The method according to claim 2, wherein a public and a secret part are separated and determined or estimated from the biometric feature.

12. (Previously Presented) The method according to claim 11, wherein the separation into a public and a secret part of the biometric feature is effected with the aid of empirical inquiries.

13. (Currently Amended) The method according to claim 12, wherein a hash value is created from the digitized biometric feature data with the aid of a hash function.

14. (Previously Presented) The method according to claim 1, wherein a hash value is created from the digitized biometric authentication feature data with the aid of a hash function.

15. (Previously Presented) The method according to claim 1, wherein the biometric feature is a behavioral biometric.

16. (Previously Presented) The method according to claim 1, wherein the biometric feature consists of a handwritten signature.

17. (Previously Presented) The method according to claim 16, wherein the handwritten signature is broken down into a public and a secret part and the secret part is a proper subset of the dynamic information of the signature.

18. (Previously Presented) The method according to claim 1, wherein the providing and/or digitizing of the biometric feature is effected several times.

19. (Previously Presented) The method according to claim 1, wherein the secret data are generated with a public-key method.

20. (Currently Amended) An apparatus for ~~carrying out the method according to claim 1~~ protecting data, comprising:

digitizing apparatus arranged to digitize a biometric feature to thereby create digitized biometric feature data;

a secret data generator comprising;

apparatus arranged to fault-tolerantly code and decode the secret data;

and

encrypting and decrypting apparatus arranged to encrypt and decrypt the fault-tolerantly coded secret data with the aid of the digitized biometric feature data;

wherein an encrypted code word is decrypted on the basis of the digitized biometric feature data, thereby obtaining a decrypted code word and;

whereby the secret data is recovered from the decrypted code word on the basis of a coding theory method with a freely selectable correction capacity.

21. (Previously Presented) The apparatus according to claim 20 including apparatus arranged to create code words.

22. (Previously Presented) The apparatus according to claim 20 including apparatus arranged to create initial correction data.

23. (Previously Presented) The apparatus according to claim 20 including apparatus arranged to provide a hash value.

24. (Previously Presented) The apparatus according to claim 20 including apparatus arranged to break down the biometric feature into a public and a secret part.

25. (Previously Presented) The apparatus according to claim 24 wherein the apparatus arranged to break down into a public and a secret part the biometric feature is further arranged to do so with the aid of statistical inquiries.

26. (Currently Amended) The apparatus according to claim 20, including apparatus arranged to capture a handwritten signature as a biometric feature.